IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

PLANO ENCRYPTION TECHNOLOGIES, LLC	§	
	§	
v.	§	Case No. 2:15-cv-1273-JRG **LEAD CASE**
	§	
AMERICAN BANK OF TEXAS, ET AL.	§	

PLAINTIFF PLANO ENCRYPTION TECHNOLOGIES, LLC'S OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Plano Encryption Technologies, LLC ("PET"), pursuant to the Patent L.R. 4-5(a), hereby submits its Opening Claim Construction Brief.

I. Introduction

PET seeks for this Court to adopt constructions taken from the language of the claims and the specification, in accordance with claim construction principles established by the Federal Circuit. In general, PET requests that the Court adopt the presumptive ordinary meaning of the claim terms, informed by the intrinsic evidence, but without rewriting the claims to include voluminous, lengthy and completely unnecessary limitations into the otherwise straightforward claim language. PET, therefore, respectfully requests that this Court adopt its proposed constructions for the terms in dispute.

II. Relevant Law

This Court is very familiar with principles of patent law, but as a brief summary of the principles relevant to this case, it is understood that "[a] claim in a patent provides the metes and bounds of the right which the patent confers on the patentee to exclude others from making, using or selling the protected invention." *Burke, Inc. v. Bruno Indep. Living Aids, Inc*., 183 F.3d 1334, 1340 (Fed. Cir. 1999). Claim construction is an issue of law for the court to decide. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970-71 (Fed. Cir. 1995) (*en banc*), *aff'd*, 517 U.S. 370 (1996).

To ascertain the meaning of claims, courts look to three primary sources: the claims, the specification, and the prosecution history. *Markman*, 52 F.3d at 979. A patent's claims must be read in view of the specification, of which they are a part. *Id.* Nonetheless, it is the function of the claims, not the specification, to set forth the limits of the patentee's invention. Otherwise, there would be no need for claims. *SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (*en banc*). Although the specification may indicate that certain embodiments are preferred, particular

embodiments appearing in the specification will not be read into the claims when the claim language is broader than the embodiments. *Electro Med. Sys., S.A. v. Cooper Life Sciences, Inc.*, 34 F.3d 1048, 1054 (Fed. Cir. 1994).

The claim construction analysis is substantially guided by the Federal Circuit's decision in *Phillips v. AWH Corporation*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). In *Phillips*, the court set forth several guideposts that courts should follow when construing claims. In particular, the court reiterated that "the claims of a patent define the invention to which the patentee is entitled the right to exclude." 415 F.3d at 1312 (internal quotations omitted). To that end, the words used in a claim are generally given their ordinary and customary meaning. *Id.* The ordinary and customary meaning of a claim term "is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, *i.e.*, as of the effective filing date of the patent application." *Id.* at 1313. This principle of patent law flows naturally from the recognition that inventors are usually persons who are skilled in the field of the invention and that patents are addressed to, and intended to be read by, others skilled in the particular art. *Id.*

Despite the importance of claim terms, *Phillips* made clear that "the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id.* Although the claims themselves may provide guidance as to the meaning of particular terms, those terms are part of "a fully integrated written instrument." *Id*. at 1315 (quoting *Markman*, 52 F.3d at 978). Thus, the *Phillips* court emphasized the specification as being the best guide for construing the claims. *Id.* at 1314-17.

Like the specification, the prosecution history helps to demonstrate how the inventor and the Patent and Trademark Office ("PTO") understood the patent. *Id*. at 1317. Because the file history,

however, "represents an ongoing negotiation between the PTO and the applicant," it may lack the clarity of the specification and thus be less useful in claim construction proceedings. *Id.* Therefore, a disclaimer found in the prosecution history requires "clear and unambiguous disavowal of claim scope." *Storage Tech. Corp. v. Cisco Sys., Inc.*, 329 F.3d 823, 833 (Fed. Cir. 2003).

III. Background of the Patents-In-Suit

Both of the patents-in-suit were originally assigned to Intel and involve methods and apparatuses used to secure communications between parties.

U.S. Patent 5,991,399 (the '399 Patent, attached as Exh. A) describes numerous embodiments of secure communication utilizing an "executable tamper resistant key module." Essentially, the patent describes various methods and apparatuses for building software modules including cryptographic keys that resists "tampering," that is, changes made either maliciously or unintentionally to the software.

In the "Statement of Reasons for Allowance" during prosecution of the application that became the '399 Patent, the examiner gave several different reasons for the allowance of the different independent claims. For example, with respect to asserted claim 1, the examiner stated:

> None of the prior art of record either taken alone or taken in any possible combination would anticipate or would tend to render obvious Applicants' claimed "method of securely distributing data" as set forth in independent claim 1 that is particularly characterized at least by the method step of "building an executable tamper key resistant identified for a selected program, the executable tamper resistant key module including the generated private key and the encrypted predetermined data" taken in the overall context of independent claim 1.

'399 FH at FH105. With respect to some of the other independent claims which were not asserted, the Examiner noted:

> None of the prior art of record either taken alone or taken in any possible combination would anticipate or would tend to render obvious Applicants' claimed "method of **distributing a conditional use private key** to a program on a remote system" as set forth in independent claim 19 . . . None of the prior art of record either taken alone or taken in any possible combination would anticipate or would tend to render obvious

> Applicants' claimed "method of **distributing a conditional use private key from a server system to a trusted player on a client system** for providing authorized access to selected encrypted digital content" as set forth in independent claim 20 . . ." (emphasis added).

Thus, the examiner recognized that, while claims 19 and 20 required distribution of a "conditional use private key," asserted claim 1 of the '399 Patent has no such limitations. Likewise, the examiner noted that unasserted claim 27 required "sending the executable tamper resistant key module ..." *See id.* Again, this limitation is not found in asserted claim 1.

In short, the teachings of the '399 Patent are quite broad. As is stated in the beginning of the specification of the '399 Patent, "[v]arious aspects of the present invention will be described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. **However, it will also be apparent to one skilled in the art that the present invention may be practiced without the specific details.** In other instances, well known features are omitted or simplified in order not to obscure the present invention." '399 Patent at 3:42-52 (emphasis added). Indeed, at the end of the '399 Patent, the inventors specifically wrote that "[i]t is important to note that although an embodiment focused on a trusted player and the secure delivery of encrypted symmetric keys has been described herein, **the methods of the present invention could be used for delivery of any data in a secure manner to a requesting program on a system served by a server.**" *Id.* at 10:40-45 (emphasis added).

U.S. Patent 5,974,550 (the '550 Patent, attached as Exh. B) relates to how to secure communications between two processes (a first and a second) running in different address spaces. Essential to understanding this patent is that the "address space" is the hardware memory addresses during the operation of a process—that is, it is all the memory actually "addressed" by a given one

or more processors during operation of a process. The '550 Patent describes how to authenticate a process running in an address space different from another address space and allowing for a more secure challenge response protocol, which is a well-known method for requesting information from a party for an appropriate response.

a. '399 Patent Asserted Claims

Plaintiff has currently asserted claims 1, 9, 10, 29 and 37 of the '399 Patent. Below are the relevant claims with the disputed language highlighted:

> 1. A method of securely distributing data comprising:
> generating **an asymmetric key pair** having a public key and a private key;
>
> encrypting **predetermined data** with the generated public key; and
>
> building an **executable tamper resistant key module** identified for a **selected program**, the **executable tamper resistant key module including the generated private key and the encrypted predetermined data**.
>
> 9. The method of claim 1, wherein building the **executable tamper resistant code module** comprises generating an **integrity verification kernel**.
>
> 10. The method of claim 9, wherein generating an **integrity verification kernel** comprises accessing an asymmetric public key of a predetermined **asymmetric key pair** associated with a manifest of the program signed by an asymmetric private key of the predetermined asymmetric key pair, producing **integrity verification kernel code** with the asymmetric public key for verifying the signed manifest of the program and combining **manifest parser generator code** and the **integrity verification kernel code** to produce the **integrity verification kernel**.
>
> 29. An apparatus for secure distribution of data comprising:
> a processor for executing programming instructions; and
> a storage medium having stored thereon a plurality of programming instructions for execution by the processor, the programming instructions generating **an asymmetric key pair** having a public key and a private key, encrypting **predetermined data** with the generated public key, and building an executable **tamper resistant key module** identified for **a program**, the executable tamper resistant key module **including the generated private key and the encrypted predetermined data**.
>
> 37. An article comprising a machine readable medium having stored therein a plurality of machine readable instructions for execution by a processing unit, the machine

readable instructions for receiving an **executable tamper resistant key module** identified for **a selected program**, the **executable tamper resistant key module including a private key of an asymmetric key pair and data encrypted by a public key of the asymmetric key pair**, for initiating execution of the **executable tamper resistant key module** to check the integrity and authenticity of the selected program and the integrity of the tamper resistant key module, and for decrypting the encrypted data with the private key when the selected program is authentic, the program's integrity is validated, and the tamper resistant key module's integrity is validated.

b. '550 Patent Asserted Claims

Plaintiff has currently asserted claims 14, 15, 16 and 17 of the '550 Patent. Below are the relevant claims with the disputed language highlighted:

14. An apparatus for authenticating a **first process** operating in an **address space** different than that of a **second process** comprising:
a processing unit for executing programming instructions; and
a storage medium having stored therein a plurality of programming instructions of the **first process** to be executed by the processing unit, wherein when executed, the plurality of programming instructions receive a **tamper resistant module** from the **second process**, initiate execution of the **tamper resistant module**, recover a secret **embedded** in the **tamper resistant module** when the integrity of the **first process** is verified during execution of the **tamper resistant** module, receive a **challenge** from the **second process**, encode the challenge using the secret to produce a response, and send the response to the **second process**.

15. The apparatus of claim 14, wherein the **tamper resistant module** comprises **integrity verification kernel** to verify the integrity of the **first process**.

16. The apparatus of claim 14, wherein the **first process** is verified when a digital signature of the **first process** determined by the **module** corresponds to a predetermined signed **manifest** of the **first process**.

17. The apparatus of claim 14, wherein the **challenge** comprises a request for information from the **first process** and the plurality of programming instructions further comprise encoding an answer to the request for information in the response.

IV. Argument for Disputed Terms

a. '399 Patent

i. an asymmetric key pair

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
one or more asymmetric key pairs, which are two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification	a matched pair of complementary cryptographic keys, wherein data encrypted by one of the keys can only be decrypted by the other key

Plaintiff's proposed construction comes straight from a federal government publication, which defines an "asymmetric key pair" as "[t]wo related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification." Glossary of Key Information Security Terms, http://infohost.nmt.edu/~sfs/Regs/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf (last visited May 15, 2016) (citing FIPS 201).

Moreover, the specification of the '399 Patent specifically teaches that private keys can be used to sign code, as well as encrypt data. *See* '399 Patent at 1:50-62:

> In modern cryptography, the security of the cryptographic algorithm (or cipher) is not dependent on keeping the algorithm secret, but instead on using a key that is kept secret. Public key cryptography uses two keys to perform cryptographic operations. One key is public and known to everyone while the second key is private and known only to a particular user. Depending on the cipher, there are two uses of public key cryptography. The first use is encryption where the public key can be used to send information that only a user with the corresponding private key can read. The second use is digital signatures where the public key is used to verify the digital signature while the private key is used to create the signature.

Defendants' construction improperly excludes a significant use for asymmetric keys that is explicitly disclosed by the specification.

The parties also dispute whether only a single asymmetric key pair is generated, or whether multiple key pairs can be used. However, the law is clear on this point. "As a general rule, the words 'a' or 'an' in a patent claim carry the meaning of 'one or more.'" *TiVo, Inc. v. EchoStar Commc'ns*

Corp., 5-16 F.3d 1290, 1303 (Fed. Cir. 2008). "The exceptions to this rule are extremely limited: a patentee must evince a clear intent to limit 'a' or 'an' to 'one.'" *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342 (Fed. Cir. 2008) (internal quotation marks and citation omitted). "The subsequent use of definite articles 'the' or 'said' in a claim to refer back to the same claim term does not change the general plural rule, but simply reinvokes that non-singular meaning." *Id*. Here, far from supporting Defendants' proposed construction, the specification in fact supports that multiple key pairs could be generated. *See* '399 Patent at 7:47 ("The key module contains a plurality of keys."); *In re 55 Brake LLC*, No. 2014-1554 at 3-4 (Fed. Cir. Apr. 13, 2015) (the plain meaning of "plurality" is "two or more").

Thus, the intrinsic and extrinsic evidence, as well as controlling Federal Circuit authority, all compel Plaintiff's proposed construction.

ii. predetermined data

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
data determined in advance of the encryption	data that has been selected for secure distribution before [generating an asymmetric key pair (claim 1) / executing the programming instructions (claim 29)]

The relevant claims require "predetermined data" to be encrypted by a public key. The ordinary meaning of this term requires only that the data be determined in advance of the encryption. *See IGT v. Bally Gaming Int'l, Inc.*, 659 F.3d 1109, 1118 (Fed. Cir. 2011) ("Again, the district court correctly construed this term. The claims and the specification only require that some condition be met in order for the system to issue the claimed command. The district court properly held that the predetermined event must be a condition chosen in advance, but there is nothing in the claims or the specification that requires the predetermined event to be finite or non-random. If the condition

determined in advance is an entirely random occurrence, it is no less an event. Bally is incorrect that this construction reads "predetermined" out of the claim. If the "predetermined event" is not "chosen in advance," the claim limitation is not met."). No claim language requires that the data must be determined prior to the generation of asymmetric key pairs or prior to the execution of any code. These limitations are improperly introduced by Defendants without any basis in the claims.

Significantly, in claim 1, the step of "generating" the one or more asymmetric key pairs occurs before the step of "building" the module with the encrypted predetermined data. While PET does not believe that the steps of the '399 Patent actually require a particular order, if an order to the steps were required, it would normally be in the order that the steps were actually claimed. *See Interactive Gift Exp., Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1342 (Fed. Cir. 2001). It would make little sense to require the determination of data before, for example, generating the asymmetric key pair, but then claiming the steps in a different order. *See E-Pass Techs., Inc. v. 3Com Corp.*, 473 F.3d 1213, 1222 (Fed. Cir. 2007) ("A method claim can also be construed to require that steps be performed in order where the claim implicitly requires order, for example, if the language of a claimed step refers to the completed results of the prior step."). Here, all that is required by the claims is that the data be determined in advance of the encryption with a public key. Defendants' construction with respect to claim 29 is even more inapt. This is an apparatus claim, and there is generally no limitation that an apparatus must be made or used in a particular order. Moreover, there is no limitation at all that the predetermined data be "distributed" at all.

iii. executable tamper resistant key module/executable tamper resistant code module/tamper resistant key module

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
software that is designed to work with other software, is resistant to modification and that	a self-contained unit of software that is capable of being communicated independently from the

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
includes a plurality of keys used for secure communication	selected program, comprising instructions to check the integrity of the selected program and itself, that is compiled to be resistant to observation and modification such that attempts to decipher what the software is doing, or modifications made to the software, will result in the software being unable to execute.

The parties agree that these different terms should be construed in the same manner. There is also little doubt that "executable" means that the key module comprises software, as proposed by all parties. *See also* '399 FH at FH84 ("Additionally, the key module is referred to as being executable. Clearly, these instances imply by context that the module is software, because if the modules were hardware, these references would not make sense.").

"Tamper resistant" also has an ordinary meaning. The meaning of "tamper" is well known. *See* Oxford Dictionary, http://www.oxforddictionaries.com/us/definition/american_english/tamper (last visited May 16, 2016) ("Interfere with (something) in order to cause damage or make unauthorized alternations."). Thus, the ordinary meaning of "tamper resistant" is not hard to fathom. *See* Dictionary.com, http://www.dictionary.com/browse/tamper-resistant?r=66 (last visited May 16, 2016) ("Difficult to tamper with.").

When claim language has as plain a meaning on an issue as the language does here, leaving no genuine uncertainties on interpretive questions relevant to the case, it is particularly difficult to conclude that the specification reasonably supports a different meaning. The specification plays a more limited role than in the common situation where claim terms are uncertain in meaning in relevant respects. The reason is that, unless there is a disclaimer or redefinition, whether explicit or implicit, the proper construction of any claim language must, among other things, "stay[] true to the claim language," and, in order to avoid giving invention-defining effect to specification language

included for other descriptive and enablement purposes, "the court's focus remains on understanding how a person of ordinary skill in the art would understand the claim terms." *Straight Path IP Grp, Inc. v. SIPNET EU SRO*, 806 F.3d 1356, 1361 (Fed. Cir. 2015).

Here, the patent discloses many methods for making the module tamper resistant. *See, e.g.,* '399 Patent at 6:7-16 ("Detailed methods for creating the tamper resistant module . . . are disclosed in pending US patent applications entitled "Tamper Resistant Methods and Apparatus," Ser. No. 08/662,679, filed Jun. 13, 1996, now U.S. Pat. No. 5,892,899 and "Tamper Resistant Methods and Apparatus," Ser. No. 08/924,740, filed Sep. 5, 1997 . . . and are incorporated herein by reference."). There is no reason to read limitations from the specification into this plain claim language. Moreover, there is nothing in this claim language that requires the program to be tamper resistant, only the module. Finally, Defendants argue that any detection of change or malicious attack must render the module "unable to execute," but this is directly contrary to the specification of the patent. '399 Patent at 5:52-55 ("[Tamper resistant software] can be trusted, within certain bounds, to operate as intended even in the presence of a malicious attack.").

The term "key module" is also used broadly in the specification. *Id.* at 7:46 ("The key module contains a plurality of keys."). During the prosecution of the '399 Patent, it was specifically argued that the meaning of the word "module" in the specification and the claims "is consistent with common usage of the word by those skilled in the art." '399 FH at FH84. This common usage is that it is software designed to work with other software. *See*, *e.g.*, '399 Patent at 7:40-41 ("The key module is forwarded over communications network 34 to client 32. It is a "plug-in" to executable 44 of trusted player 42."). Moreover, Defendants' proposed construction of a module as a "self-contained unit of software" has no actual technical meaning in the context of software, while the added limitation that the module must be "capable of being communicated independently from the selected program"

improperly incorporates limitations not provided by the claims, that together simply do more to confuse rather than clarify the scope of the disclosed invention. The claim language explains what keys are necessary to be included in the module and, thus, Plaintiff's proposed construction of the term is clear. There is no reason to dangle a paragraph of additional limitations derived from these few words, like adding ornaments to a Christmas tree, in accordance with the Defendants' proposed construction.

Indeed, the number of additional limitations to this claim language proposed by Defendants is astounding. According to the Defendants, the key module must be "a self-contained unit" "that is capable of being communicated independently from the selected program, comprising instructions to check the integrity of the selected program and itself, that is compiled to be resistant to observation and modification such that attempts to decipher what the software is doing, or modifications made to the software, will result in the software being unable to execute." None of these additional limitations are found in the meaning of the claim language. Defendants' arguments should be rejected. *AllVoice Computing PLC v. Nuance Commc'ns, Inc.*, 504 F.3d 1236, 1248 (Fed. Cir. 2007) ("[E]very claim need not contain every feature taught in the specification."); *Nazomi Commc'ns, Inc. v. ARM Holdings, PLC*, 403 F.3d 1364, 1369 (Fed. Cir. 2005) (holding that claim may "embrac[e] different subject matter than is illustrated in the specific embodiments in the specification").

As noted above, many of these limitations appear to be an attempt to read limitations from other independent and dependent claims into broader claim language, and should be rejected for that reason as well. "Differences among claims can . . . be a useful guide in understanding the meaning of particular claim terms." *Phillips*, 415 F.3d at 1314. "[T]he context in which a term is used in the asserted claim can be highly instructive." *Id.*

iv. selected program/program

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
ordinary meaning; a "program" is a series of computer instructions; selected program means a "particular series of computer instructions"	an application program

"Program" has an ordinary meaning, and is one of the most common words used in software. Oxford Dictionary, http://www.oxforddictionaries.com/us/definition/american_english/program (last visited May 15, 2016) ("A series of coded software instructions to control the operation of a computer or other machine."); Macmillan Dictionary, http://www.macmillandictionary.com/dictionary/american/program_1#program_1__5 (last visitied May 15, 2016) ("A series of instructions that makes a computer perform an action or a particular type of work".); Computer, Telephony & Electronics Industry Glossary, http://www.csgnetwork.com/glossaryp.html#program (last visited May 15, 2016) ("A series of instructions that tell a computer what to do."). Defendants' proposed construction improperly limits the plain meaning of "program" to a particular type of program contrary to its ordinary meaning. If the inventors of the '399 Patent had meant to limit their claims to "application program" (whatever Defendants may propose by inserting the term "application"), they would have modified the claim language in such a manner. Redefinition or disavowal is required where claim language is plain, lacking a range of possible ordinary meanings in context. *See Pacing Technologies, LLC v. Garmin Int'l, Inc.*, 778 F.3d 1021, 1024 (Fed. Cir. 2015) (citing authorities).

Moreover, the inventors use the term "program" in the specification in its ordinary sense, and at times distinguish between an "application program" -- for example, '399 Patent at 2:35-37 ("Consider the situation where an application program running on a user's PC accesses encrypted digital content on a storage medium") -- and simply a "program" -- for example, *id*. at 3:5-6 ("An embodiment of the present invention is a method of securely distributing data to a program on a

remote system."). There is simply no reason or justification to read in the additional limitation of an "application program" into this plain claim language. "[I]t is improper to read limitations from a preferred embodiment described in the specification—even if it is the only embodiment—into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited." *Liebel-Flarsheim v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004).

v. including the generated private key and the encrypted predetermined data/including a private key of an asymmetric key pair and data encrypted by a public key of the asymmetric key pair

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
including one or more of the private keys of the one or more asymmetric key pairs and encrypted predetermined data	has compiled within itself the encrypted predetermined data, and the private key that can be used to decrypt the encrypted predetermined data
including one of the private keys of one or more asymmetric key pairs and data encrypted by one of the public keys of one or more asymmetric key pairs	has compiled within itself data encrypted by a public key, and the private key that can be used to decrypt said data

Other than understanding the meaning of the terms "private key" and "public key," which both have ordinary meanings in the art,[1] the primary dispute between the parties on these claims terms center on the meaning of the word "including." Plaintiff's construction of this term is consistent with Federal Circuit precedent as the Federal Circuit has held that this claim term "including" is synonymous with "comprising," and should be given a broad construction. *Hewlett-Packard Co. v.*

[1] Private Key: "The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data." Glossary of Key Information Security Terms, http://infohost.nmt.edu/~sfs/Regs/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf (last visited May 15, 2016) (citing SP 800-63). Public Key: "The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data." *Id.*

Repeat-O-Type Stencil Mfg. Corp., 123 F.3d 1445, 1451 (Fed. Cir. 1997) (the claim term "including" is synonymous with "comprising"). The specification and prosecution history only compel departure from the plain meaning of a term in two narrow instances not applicable here: lexicography and disavowal. *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012). Since nothing in the '399 Patent's specification or prosecution history explicitly defines the term "including" to mean "compiled within," or disavows its normal broad scope, Plaintiff's construction should be adopted.

The parties further dispute whether the relevant claim language limits itself to only a single asymmetric key pair. Contrary to Defendants' construction, the claims require nothing more than including a private key. Including a private key to sign the key module as part of the building step is specifically disclosed as preferred embodiments in the specification. *See* '399 Patent at 7:46-51 ("The key module contains a plurality of keys. It contains an asymmetric public key for verifying the digital signature of the manifest. The digital signature was created using an asymmetric private key by the manufacturer of the trusted player."); *Id.* at 10:35-39 ("The signature verification engine function is performed on the digest of the specified object using the generated asymmetric private key to generate a signature, which can be validated by the trusted player or other application on the client."). Defendants' construction that "including" be limited to "compiled within" would exclude this preferred embodiment. "[A] claim construction that excludes a preferred embodiment . . . is rarely, if ever correct and would require highly persuasive evidentiary support." *See Anchor Wall Sys., Inc. v. Rockwood Retaining Walls, Inc.*, 340 F.3d 1298, 1308 (Fed. Cir. 2003) (citations omitted).

This use of a private key of a generated asymmetric key pair to sign the software is specifically covered by dependent claims. Claim 9 recites, "[t]he method of claim 1, wherein building the executable tamper resistant code module comprises generating an integrity verification kernel."

Claim 10 then explains that "generating an integrity verification kernel" may comprise "a manifest of the program signed by an asymmetric private key of the predetermined asymmetric key pair." Thus, while not required by claim 1, certainly using a private key (of one of the generated asymmetric key pairs) to sign a manifest of the program is within the scope of the claims.

While there are other dependent claims that cover different embodiments of the inventions, such as using a private key to decrypt the encrypted predetermined data (see, for example, dependent claim 4)[2], there is no reason to read these limitations into claim 1, much less exclude the embodiments found in claim 10. The doctrine of claim differentiation "normally means that limitations stated in dependent claims are not to be read into the independent claim from which they depend." *Karlin Tech., Inc. v. Surgical Dynamics, Inc.*, 177 F.3d 968, 971-72 (Fed. Cir. 1999) (stating that this interpretative tool stems from "the common sense notion that different words or phrases used in separate claims are presumed to indicate that the claims have different meanings and scope"); *see also Phillips*, 415 F.3d at 1314-15 ("[T]he presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim."); *Ecolab Inc. v. Paraclipse, Inc.*, 285 F.3d 1362, 1375 (Fed. Cir. 2002) (presumption is especially strong when the limitation in dispute is the only meaningful difference between an independent and dependent claim, and one party is urging that the limitation in the dependent claim should be read into the independent claim).

The requirement of "distributing a conditional use private key" incorporated into Defendants' constructions are both elements of other independent claims. As noted above, the examiner specifically noted these differences between the independent claims in the statement given for the

[2] Claim 4 reads "[t]he method of claim 3, further comprising decrypting the encrypted predetermined data with the generated private key for the tamper resistant key module when the program is authentic and the program's integrity is validated and the tamper resistant key module's integrity is validated."

reasons for allowance. *See* '399 FH at FH105. If these were elements required of all claims, it would make no sense to have these limitations in only some claims. *See Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1326 (Fed. Cir. 2003) ("Our court has made clear that when a patent claim 'does not contain a certain limitation and another claim does, that limitation cannot be read into the former claim in determining either validity or infringement.'").

vi. integrity verification kernel

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
software that can be used in conjunction with other software to determine that code has not been altered through the use of a digital signature	a small code segment that is compiled in a manner to make it resistant to observation and modification, such that attempts to decipher what the software is doing, or modifications made to the software, will result in the software being unable to execute and that verifies that the image of the program corresponds to a supplied digital signature for that program

All parties agree that the integrity verification kernel comprises software. "Integrity" has a well-known meaning in the art of encryption. Glossary of Key Information Security Terms, http://infohost.nmt.edu/~sfs/Regs/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf (last visited May 15, 2016) (citing FIPS 140-2) ("The property that data has not been altered in an unauthorized manner."); Netlingo Dictionary, http://www.netlingo.com/word/integrity.php ("Commonly referred to as "data integrity," this form of cryptography makes sure that the data you received has not been modified since it was sent.") This meaning is supported by the specification. *See, e.g.,* '399 Patent at 1:27-29; 2:30-35; 3:14-17; 3:53-59; 4:8-14; 4:18-20; 4:56-59; 5:15-17 "Verification" also has a well-known meaning in the art. Oxford Dictionary, http://www.oxforddictionaries.com/us/definition/american_english/verification (last visited May 15, 2016) ("The process of establishing the truth, accuracy, or validity of something."); Webster's New

Work College Dictionary, http://www.yourdictionary.com/verification (last visited May 15, 2016) ("A verifying or being verified; establishment or confirmation of the truth or accuracy of a fact, theory, etc."); Dictionary.com, http://www.dictionary.com/browse/verification?r=66 (last visited May 15, 2016) ("Evidence that establishes or confirms the accuracy or truth of something.").

Although various embodiments are described in the specification for the "integrity verification kernel" (or "IVK" as it is commonly abbreviated in the specification), the specification describes an IVK as "software that verifies that a program image corresponds to the supplied digital signature." '399 Patent at 5:18-20. The specification also explains that an IVK "can be used alone . . . or it can be used in conjunction with other software. . . ." *Id.* at 5:22-24. These aspects of the IVK are incorporated in Plaintiff's construction. Defendants' construction unnecessarily incorporates its construction for the different claim term "tamper resistant" into its construction for the IVK.

Again, the remainder of Defendants' proposed construction appears to be reading limitations regarding specific IVKs described in the specification into the claims, and should be rejected. *Superguide Corp. v. DirecTV Enterprises, Inc.,* 358 F.3d 870, 875 (Fed. Cir. 2004). For example, there is nothing that requires that the code be unable to operate in the event of a change or "an attempt to decipher what the software is doing." To the contrary, the specification teaches that "tamper resistant" software is often designed to continue to operate even in the event of a detected attack, much less when one attempts to decipher what the software is doing. '399 Patent at 5:52-55 ("Tamper resistant software . . . can be trusted, within certain bounds, to operate as intended even in the presence of a malicious attack."). *See* Section IV-a(iii), *supra.*

vii. integrity verification kernel code

Plaintiff's Proposed Construction	Defendants' Proposed Construction
source code that can be used in conjunction with other software to determine that code has not been altered through the use of a digital signature	source code for calculating digital signatures that is generated using the asymmetric public key for the manifest of the selected program

Essentially, all parties agree that "integrity verification kernel code" is source code for the IVK. However, the specification describes creating digital signatures using private keys. '399 Patent at 2:60-62 ("The second use is digital signatures where the public key is used to verify the digital signature while the private key is used to create the signature."). Defendants' construction requires that the digital signature is generated using "*an asymmetric public key* for the manifest of the selected program" and not a private key and thus excludes this embodiment of the disclosed invention. There is no reason this preferred embodiment should be excluded. "A claim interpretation that excludes a preferred embodiment from the scope of the claim is rarely, if ever, correct." *Accent Packaging, Inc. v. Leggett & Platt, Inc.*, 707 F.3d 1318, 1326 (Fed. Cir. 2013) (internal citation omitted).

viii. manifest

Plaintiff's Proposed Construction	Defendants' Proposed Construction
code and/or data that contains metadata describing other code	a data file containing a statement regarding the integrity and authenticity of a specific installation of the selected program comprising a unique identifier for that specific installation and its corresponding digital signature

"Manifest" has a well-known meaning in the software art. Your Dictionary, http://www.yourdictionary.com/manifest (last visited May 15, 2016) ("A file containing metadata describing other files."); Wikipedia, https://en.wikipedia.org/wiki/Manifest_file (last visited May 15, 2016) ("A manifest file in computing is a file containing metadata for a group of accompanying files that are part of a set or coherent unit."). Essentially, in software, a "manifest" is like a ship's manifest

—it describes what is inside code, the way a ship's manifest describes what is inside the ship. Although the specification describes various attributes of embodiments of the manifest in the invention, there is no reason to read these limitations from the specification into the claims. *AllVoice Computing*, 504 F.3d at 1248 ("[E]very claim need not contain every feature taught in the specification."); *Nazomi*, 403 F.3d at 1369 (claims may "embrac[e] different subject matter than is illustrated in the specific embodiments in the specification").

ix. manifest parser generator code

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
manifest source code which can be compiled so the manifest can be used	static source code that includes the integrity verification kernel's entry code, generator code, accumulator code, and other code for tamper detection

This term is also somewhat self-explanatory. The purpose of the manifest is to describe code. While there must be code which can be compiled so that the manifest can perform its function, there is no claim requirement limiting that code to any particular type. *See, e.g.*, '399 Patent at 9:51-54 ("The generated 'C' IVK source code for the key module 210 and the manifest parser generator source code 212 are combined into the single IVK source code module 206."). While, for example, this code is described as being in the "C" programming language in the preferred embodiments, there is no reason to read this limitation from the specification into the claims, any more than there is any reason to read the laundry list of limitations that Defendants want to add to the straightforward language of the claims.

b. '550 Patent

i. address space

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
memory used by one or more processor(s) during operation	all memory locations available to a process

The ordinary meaning of the term "address space" is "the range of memory [a processor] uses while running." Computer User High Tech Dictionary, http://www.computeruser.com/dictionary?name-directory-search-value=address (last visited May 15, 2016) ("The address space of a program or process is the range of memory it uses while running."); Dictionary of Engineering, http://www.dictionaryofengineering.com/definition/address-space.html (last visited May 15, 2016) ("The actual memory used while running a computer program.").

Thus, the invention of the '550 Patent involves a first and second process that are running on different memory spaces during operation, in accordance with the ordinary meaning of the term, as confirmed by the specification. '550 Patent at 25-34 ("It would be better if one party could authenticate the other party to ensure that the other party has not be tampered with or 'hacked,' as opposed to just validating that the other party shares the secret. This can be done when the parties share the same address space by checking the contents of memory of the other party, computing its digital signature, and verifying its integrity. However, this cannot be accomplished across different process address spaces unless the memory is shared.") (emphasis added).

However, an address space is not the entire range of memory potentially "available" to a process as Defendants contend. Instead, it is the memory actually *used* by a process. '550 Patent at 2:18-20 ("These processes do not share an address space and may or may not exist on the same processor or computer system."). Figure 3 of the '550 Patent, reproduced below, shows the hardware for a computer system:

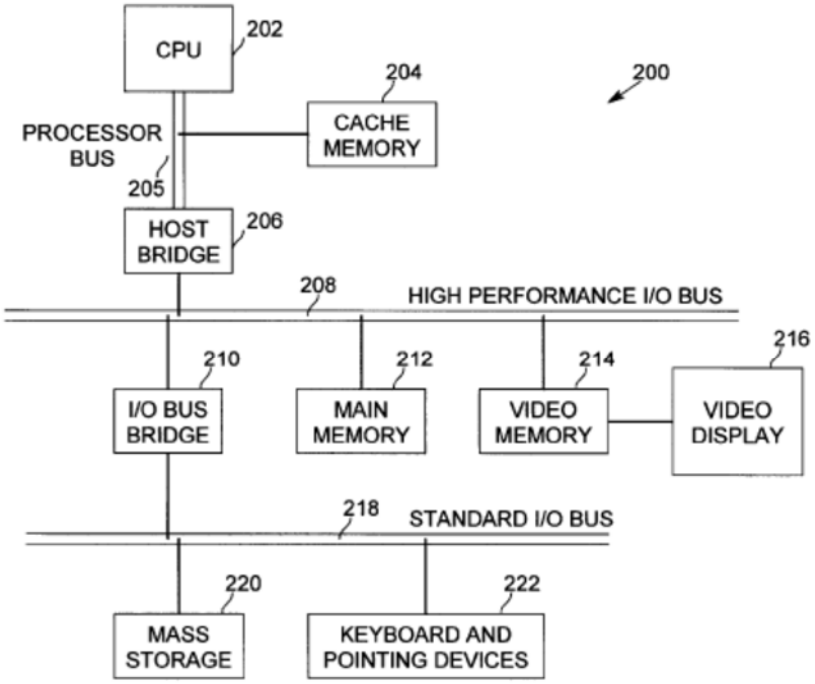

FIG. 3

The '550 Patent explains: "FIG. 3 illustrates a sample computer system suitable to be programmed with the authentication method in accordance with embodiments of the present invention. Sample computer system 200 may be used to execute processing steps described above for Process A, Process B, or both. When Process A and Process B are on systems remote from each other, Process A is executing on a first sample computer system and Process B is executing on a second sample computer system connected to the first sample computer system via a network." '550 Patent 4:61-5:3. In other words, the patent discloses that the same computer system sharing the same potentially available range of memory may be used to execute processing steps for both Process A and Process B.

Therefore, what is required is that the first and second process be actually running in different memory spaces during operation, not that the first and second process could not (in theory) access the memory of the other. Otherwise, it would not be possible to describe different processes running

on the same computer as being in different address spaces, since all the memory for the computer would be "available" to the processes.

ii. first process/second process

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
a series of actions or steps running in different address spaces from the second process	an instance of a computer program that is executing within a specific address space that is different from the address space of the second process
a series of actions or steps running in different address spaces from the first process	an instance of a computer program that is executing within a specific address space that is different from the address space of the first process

The claim term "process" is intended to be conceptually different from a "program." If the inventors of the '550 Patent—computer experts at Intel—had wanted to limit the claims to an instance of a computer program, this language would have been readily available and known to them. Instead, the inventors used the term "process," and the ordinary meaning of that term should apply. While the steps of the claimed first and second processes must run on processors, they need not be part of a single "program." The patentee's lexicography must govern the claim construction analysis. *Phillips*, 415 F.3d at 1316.

Defendants' proposed rewriting of the claim term "process" is improper. "In construing claims, the analytical focus must begin and remain centered on the language of the claims themselves, for it is that language that the patentee chose to use to 'particularly point[] out and distinctly claim[] the subject matter which the patentee regards as his invention.'" *Interactive Gift Express, Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1331 (Fed. Cir. 2001) (quoting 35 U.S.C. § 112, ¶ 2 (1975), amended by 35 U.S.C. § 112(b)).

Moreover, the '550 Patent specification definitively rejects the notion that a process must be an instance of a single computer program: "In particular, mass storage 220 is used to provide permanent storage for **the executable instructions of the authentication and tamper resistant programs/applications**, whereas main memory 212 is used to temporarily store the executable instructions of **authentication and tamper resistant programs/applications during execution by CPU 202**. While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the inventions pertains are deemed to lie within the spirit and scope of the invention." '550 Patent at 5:15-29. Thus, the specification explicitly discloses that the series of steps that make up the first and second process need not be limited to a single computer program much less an instance of one but can come from multiple "programs/applications" so long as the steps of the process are met.

Thus, the "process" should not be limited to "an instance of a computer program" as such a construction is specifically contrary to broad description of a "process" in the specification. "[A] claim construction that excludes a preferred embodiment . . . is rarely, if ever correct and would require highly persuasive evidentiary support." *Anchor Wall*, 340 F.3d at 1308 (citations omitted).

iii. tamper resistant module/module

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
software that is designed to work with other software and that is resistant to modification	a self-contained unit of software that is capable of being communicated independently from the selected program, comprising instructions to check the integrity of the selected program and itself, that is compiled to be resistant to observation and modification such that attempts to decipher what the software is doing, or

Plaintiff's Proposed Construction	Defendants' Proposed Construction
	modifications made to the software, will result in the software being unable to execute.

With respect to the '550 Patent, there is no discussion of particular cryptographic keys in the module, but rather an embedded secret that is recovered when the module is executed, or run, by a processor. Otherwise, the construction is very similar to the '399 Patent, and the arguments set forth above apply equally here and are therefore incorporated herein. *See* Section IV-a(iii), *supra.* Just as in the '399 Patent, there is no reason to read additional limitations into the ordinary meaning of the term "tamper resistant." Just as in the '399 Patent, tamper resistant software modules do not necessarily stop executing because tampering is detected. '550 Patent at 2:49-52 ("Tamper resistant software . . . can be trusted, within certain bounds, to operate as intended even in the presence of a malicious attack."). Constructions which exclude these embodiments should be rejected.

Moreover, just as in the '399 Patent, there is also no reason to read additional limitations into the word "module," which is used broadly in the specification. *See, e.g.*, '550 Patent at 3:14-19 ("Two interprocess software modules requiring to communicate with each other can establish that the module one is calling is indeed the one it is expecting by computing the digital signature of the called module and comparing the computed signature against a predetermined value."); '550 Patent at 3:30-32 ("The tamper resistant module 14 also contains a secret 16 which the tamper resistant module will not divulge until the integrity verification for Process B 12 is a success."). *AllVoice Computing*, 504 F.3d at 1248 ("[E]very claim need not contain every feature taught in the specification."); *Nazomi*, 403 F.3d at 1369 (claims may "embrac[e] different subject matter than is illustrated in the specific embodiments in the specification").

iv. embedded

Plaintiff's Proposed Construction	Defendants' Proposed Construction
made an integral part of	compiled within

"Embedded" has an ordinary meaning. Collins Dictionary, http://www.collinsdictionary.com/dictionary/english/embedded (last visited May 17, 2016) ("Made an integral part of other software."); Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/embed (last visited May 17, 2016) ("To make something an integral part of"). That ordinary meaning was used during prosecution of the '550 Patent. *See* '550 FH at FH199 ("Neither Berry nor Penzias teach or suggest that a key used to encode a response to a challenge may be embedded within a tamper resistant module, and that the key is accessible only after integrity verification of the remote process is performed."). Thus, "embedded," consistent with its ordinary meaning, means that a secret (whether a key or otherwise) is an integral part of the tamper resistant module. This meaning is also supported by the language of claim 14 – "recover a secret embedded in the tamper resistant module when the integrity of the first process is verified during execution of the tamper resistant module."

Defendants do not explain what is meant by "compiled within," but that is not normally a meaning ascribed to the word "embedded," and appears to be an attempt to improperly limit the claim scope. *See Phillips*, 415 F.3d at 1314-17; *Interactive Gift*, 256 F.3d at 1331.

v. challenge

Plaintiff's Proposed Construction	Defendants' Proposed Construction
prompt for information to authenticate a user	arbitrary data known to the second process and unknown to the first process until received from the second process

The word "challenge" has an ordinary meaning in the software art. Webopedia,

http://www.webopedia.com/TERM/C/challenge_response.html (last visited May 15, 2016) ("A common authentication technique whereby an individual is prompted (the challenge) to provide some private information (the response)."); Techopedia, https://www.techopedia.com/definition/26138/challenge-response-authentication (last visited May 15, 2016) ("Challenge-response authentication is a group or family of protocols characterized by one entity sending a challenge to another entity. The second entity must respond with the appropriate answer to be authenticated."). The inventors adopted this "well-known" meaning during the prosecution of the '550 Patent. *See*, *e.g.*, '550 FH at FH198 ("Penzias discloses a simple variation on a well-known challenge/response protocol whereby a human requester must supply a selected one of several previously provided and stored pieces of information in order to participate in a credit card transaction."). This simply appears to be yet another attempt by the Defendants to improperly rewrite claim language. *Interactive Gift*, 256 F.3d at 1331.

vi. integrity verification kernel

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
software that can be used in conjunction with other software to determine that code has not been altered through the use of a digital signature	a small code segment that is compiled in a manner to make it resistant to observation and modification, such that attempts to decipher what the software is doing, or modifications made to the software, will result in the software being unable to execute and that verifies that the image of the program corresponds to a supplied digital signature for that program

As discussed above with respect to the '399 Patent in Section IV-a(vi), although various embodiments are described in the specification for the "integrity verification kernel" (or "IVK" as it is commonly abbreviated in the specification), the specification describes an IVK as "software that verifies that a program image corresponds to the supplied digital signature." '550 Patent at 3:4-6.

This description is supported by the ordinary meaning of the terms, as described above. These arguments are further supported by the prosecution history for the '550 Patent. '550 FH at FH197 ("The present invention also determines the integrity of the remote process, to detect if it has been tampered with, through the use of an integrity verification kernel.").

vii. manifest

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
code and/or data that contains metadata describing other code	a data file containing a statement regarding the integrity and authenticity of a specific installation of the selected program comprising a unique identifier for that specific installation and its corresponding digital signature

Just as for the '399 Patent, the term "manifest" has an ordinary meaning that should be presumptively adopted for its construction in the claims. The same arguments raised with respect to construction of this term for the '399 patent are incorporated herein. *See* Section IV-a(vii), *supra.*

V. Conclusion

PET respectfully requests the Court adopt its proposed constructions.

Respectfully Submitted,

/s/ Papool S. Chaudhari

Dated: May 17, 2016 By: _____

Jeremy S. Pitcock
PITCOCK LAW GROUP
1501 Broadway, 12th Floor
New York, NY 10036
(646) 571-2237
(646) 571-2001 Fax
jpitcock@pitcocklawgroup.com

Papool S. Chaudhari
Texas State Bar No. 24076978
CHAUDHARI LAW, PLLC
P.O. Box 1863

Wylie, Texas 75098
Phone: (214) 702-1150
Fax: (214) 705-3775
Papool@ChaudhariLaw.com

ATTORNEYS FOR PLAINTIFF
PLANO ENCRYPTION TECHNOLOGIES, LLC

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule CV-5(a). As such, the foregoing was served on all counsel of record who have consented to electronic service. Local Rule CV-5. Pursuant to Fed. R. Civ. P. 5(d) and Local Rule CV-5, all others not deemed to have consented to electronic service will be served with a true and correct copy of the foregoing via email on this 17th day of May, 2016.

/s/ Papool S. Chaudhari

Papool S. Chaudhari